UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/522,919	01/31/2005	Paul W Hodgson	36-1885	4217

23117 7590 05/21/2010

NIXON & VANDERHYE, PC
901 NORTH GLEBE ROAD, 11TH FLOOR
ARLINGTON, VA 22203

EXAMINER	
TAHA, SHAQ	
ART UNIT	PAPER NUMBER
2446	

MAIL DATE	DELIVERY MODE
05/21/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/522,919	HODGSON, PAUL W	
	Examiner	Art Unit	
	SHAQ TAHA	2446	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 February 2010*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1 - 10, 12 - 18, 20, and 22 - 37* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1 - 10, 12 - 18, 20, and 22 - 37* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *02/24/2010, 04/30/2010*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This is a final action for application number 10/522,919 after a non-final filed on 02/23/2010. The original application was filed on 01/31/2005. Claim 1, 12, 20, 23, 31, 35, and 36 are amended. Claims 1 – 10, 12 – 18, 20, 22 – 31, and 33 - 37 are currently pending and have been considered below. Claims 11, 19, 21, and 23 are cancelled. Claims 1, 12, 20, 23, 31, 32, 36 and 37 are independent claims.

Applicant's Response

Applicant's arguments with respect to claims 1 – 10, 12 – 18, 20, 22 – 31, and 33 - 37 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1 - 4, 8 - 10, 12 - 15, 22 - 24, 31, 33, 34, 36, and 37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Paul et al. (US 6,052,709), in view of Barrett et al. (US 2002/0059454

Regarding claims 1, 12, 22, 23, and 36, Paul et al. an apparatus comprising: at least one server configured to send outgoing electronic messages on behalf of terminals

connected thereto and to deliver incoming electronic messages to the terminals, each terminal being accessed by one or more users, **[A plurality of network servers 120, 121, and 122 are coupled to the control center 101 and the communications network 110 as shown in Fig. 1, wherein the servers are mail servers, (Paul et al., Col. 3, lines 57 – 62)],**

the server comprising: means arranged to generate or receive traffic log data based on at least one traffic characteristic using data derived from the handling of plural electronic messages, **[Once the information contained in the received e-mail message is identified and received by processor 104, wherein the received e-mail contains information that is used to filter the e-mails based on the information received, (Paul et al., Col. 5, lines 1 - 6)],**

analyzing means arranged to analyze the traffic log data as a function of a predetermined traffic characteristic criterion corresponding to malicious electronic message traffic to identify electronic messages that satisfy the traffic characteristic criterion, **[Upon receipt of incoming mail addressed to the spam probe addresses, the spam control center automatically analyzes the received mail to identify the source of the message, extracts and processes the source data from the received message, wherein the received message is analyzed based on the characteristics that meet the criterion of a spam message, (Paul et al., Col. 2, lines 1 – 5)],**

identifying means arranged to identify the destination of the identified electronic messages, **[users and/or service providers may optionally implement filtering based upon additional exclusion list categories, such as the "TO", "BCC," "CC,"**

and "SUBJECT" e-mail headers and other headers. Filtering may also be based on the contents in the body of the email, wherein the "to" identifies the destination, (Paul et al., Col. 6, lines 7 – 12)],

and processing means arranged to send a control message to each of the identified destinations, **[generating an alert signal incorporating the extracted source data, (Paul et al., Col. 10, lines 4 – 6)],**

requesting suspension of delivery of the identified electronic messages, **[messages marked with the first display code indicating the "JUNK" status of the message are not displayed in the user's in-box and are automatically discarded by the filter, wherein the alert message discards the electronic message, (Paul et al., Col. 6, lines 65 – 67)],**

Paul et al. fails to teach that the traffic characteristic criterion including the number of electronic messages from a common user, terminal or other topological position within a time interval,

Barrett et al. teaches determining whether the electronic data has characteristics of spam may also include counting a number of communications of electronic data that have been received from the sender during a period of time, **(Barrett et al., Paragraph 6)**, in order to determine that the electronic data has characteristics of spam to be blocked when the number of messages received from the sender exceeds a threshold number during the period of time, **(Barrett et al., Paragraph 6),**

It would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify Paul et al. by including that the traffic characteristic

criterion including the number of electronic messages from a common user, terminal or other topological position within a time interval, **(Barrett et al., Paragraph 6)**, in order to determine that the electronic data has characteristics of spam to be blocked when the number of messages received from the sender exceeds a threshold number during the period of time, **(Barrett et al., Paragraph 6).**

Regarding claims 2 and 13, an apparatus wherein said server includes: first means arranged to receive a signal identifying whether or not an identified electronic message is related to an electronic message virus, **[and generates an alert signal containing the spam source data, (Paul et al., Abstract)],**

and second means arranged to receive data indicative of the success or otherwise of the control message and, in the event that the received signal identifies an electronic message to be a virus and the control message is successful, to trigger deletion of the said identified electronic message, **[The filtering system controls delivery of the unsolicited e-mail messages by discarding the messages without displaying them to the user, (Paul et al., Col. 2, lines 17 – 20)].**

Regarding claims 3 and 14, an apparatus wherein: in the event that a received signal identifies an electronic message to be a virus and the control message is unsuccessful, the second means is arranged to trigger operation of identifying means and processing means running on a second server corresponding to the destination of the identified electronic message, **[A plurality of network servers 120, 121, and 122**

are coupled to the control center 101 and the communications network 110. User terminals 130-138 are respectively coupled to servers 120-122 as shown in FIG. 1, (Paul et al., Col. 3, lines 59 - 63)].

Regarding claim 4 and 15, an apparatus server wherein: in the event that a received signal identifies an electronic message not to be a virus and the control message is successful, the second means is arranged to permit delivery of the identified electronic message, **[A method for controlling delivery of unsolicited electronic mail, (Paul et al., Col. 2, lines 62 – 65)].**

Regarding claim 8, an apparatus for delivering electronic messages, comprising a plurality of apparatus wherein at least one of the therein servers comprises: receiving means arranged to receive a request to suspend delivery of an identified electronic message, **[messages marked with the first display code indicating the "JUNK" status of the message are not displayed in the user's in-box and are automatically discarded by the filter, wherein the alert message discards the electronic message, (Paul et al., Col. 6, lines 65 – 67)],**

and wherein, in response to receipt of a said request, polling means is arranged to check delivery of the identified electronic message, and in the event that it has not been delivered, to block retrieval thereof, **[A method for controlling delivery of unsolicited electronic mail, (Paul et al., Col. 2, lines 62 – 65)].**

Regarding claim 9, an apparatus wherein: the at least one server includes deleting means for deleting an electronic message, **[The filtering system controls delivery of the unsolicited e-mail messages by discarding the messages without displaying them to the user, (Paul et al., Col. 2, lines 17 – 20)]**,

and in response to receipt of a signal identifying that an identified electronic message is related to an electronic message virus, the deleting means is arranged to check whether retrieval of the identified electronic message has been blocked, and if it has, to delete it, **[The filtering system controls delivery of the unsolicited e-mail messages by discarding the messages without displaying them to the user, (Paul et al., Col. 2, lines 17 – 20)].**

Regarding claim 10, an apparatus wherein: in the event that the identified electronic message is related to an electronic message virus, and the identified electronic message has not been blocked, the server is arranged to invoke its identifying means and processing means in respect of electronic messages sent by the identified destinations, **[the spam control center automatically analyzes the received mail to identify the source of the message, extracts and processes the source data from the received message, (Paul et al., Col. 2, lines 2 – 6)].**

Regarding claim 24, a server according to claim 23, the server comprising:

identifying means arranged to identify the destination of said identified electronic messages, **[users and/or service providers may optionally implement filtering**

based upon additional exclusion list categories, such as the "TO", "BCC," "CC," and "SUBJECT" e-mail headers and other headers. Filtering may also be based on the contents in the body of the email, wherein the "to" identifies the destination, (Paul et al., Col. 6, lines 7 – 12)],

and processing means arranged to send a control message to each of the identified destinations requesting suspension of delivery of the identified electronic messages, **[messages marked with the first display code indicating the "JUNK" status of the message are not displayed in the user's in-box and are automatically discarded by the filter, wherein the alert message discards the electronic message, (Paul et al., Col. 6, lines 65 – 67)].**

Regarding claims 31, a tangible computer-readable storage medium having a computer program thereon for sending and receiving electronic messages, the program being executable on a terminal having a user interface, **[A user interface 208 is provided to receive inputs from the user and to display e-mail information to the user, (Paul et al., Col. 6, lines 32 – 35)],**

the computer program being configured to perform the following steps when executed: (a) invite a user to input at the user interface send instructions for sending one or more electronic messages, **[A plurality of network servers 120, 121, and 122 are coupled to the control center 101 and the communications network 110 as shown in Fig. 1, wherein the servers are mail servers, (Paul et al., Col. 3, lines 57 – 62)],**

(b) determine if traffic log data based on handling a plurality of electronic messages meets a predetermined traffic characteristic criterion corresponding to malicious electronic message traffic, **[Upon receipt of incoming mail addressed to the spam probe addresses, the spam control center automatically analyzes the received mail to identify the source of the message, extracts and processes the source data from the received message, wherein the received message is analyzed based on the characteristics that meet the criterion of a spam message, (Paul et al., Col. 2, lines 1 – 5)],**

(c) if the criterion is met, invite the user to input at the user interface a confirmation input to confirm the send instructions, **[upon receipt of an electronic mail message addressed to the probe address, (Paul et al., Col. 2, lines 57 – 60)],**

(d) upon receipt of the confirmation input, transmit the electronic messages from the terminal, **[generating an alert signal incorporating the processed source data, (Paul et al., Col. 2, lines 60 – 62)],**

and (e) transmit authentication data associable with the transmitted electronic messages, **[The network users may or may not be given authorization to access or change the exclusion list data entered by the system operator, (Paul et al., Col. 9, lines 52 – 55)]**

Paul et al. fails to teach that the traffic characteristic criterion including the number of electronic messages from a common user, terminal or other topological position within a time interval,

Barrett et al. teaches determining whether the electronic data has characteristics of spam may also include counting a number of communications of electronic data that have been received from the sender during a period of time, **(Barrett et al., Paragraph 6)**, in order to determine that the electronic data has characteristics of spam to be blocked when the number of messages received from the sender exceeds a threshold number during the period of time, **(Barrett et al., Paragraph 6),**

It would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify Paul et al. by including that the traffic characteristic criterion including the number of electronic messages from a common user, terminal or other topological position within a time interval, **(Barrett et al., Paragraph 6)**, in order to determine that the electronic data has characteristics of spam to be blocked when the number of messages received from the sender exceeds a threshold number during the period of time, **(Barrett et al., Paragraph 6).**

Regarding claim 33, Paul et al. teaches a plurality of network servers 120, 121, and 122 are coupled to the control center 101 and the communications network 110 as shown in Fig. 1, **(Paul et al., Col. 3, lines 57 – 62),**

Paul et al. fails to teach that the terminal is configured to transmit the authenticating data in encrypted form,

Steiger et al. teaches that encryption may provide data confidentiality, while still allowing flexibility in the client and server application, **(Steiger et al., Col. 10, lines 63 -**

67), in order to adequately protect computer information assets on a full-time basis, **(Steiger et al., Col. 1, lines 47 – 50),**

It would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify Paul et al. transmitting the authenticating data in encrypted form, **(Steiger et al., Col. 10, lines 63 - 67)**, in order to adequately protect computer information assets on a full-time basis, **(Steiger et al., Col. 1, lines 47 – 50).**

Regarding claims 34, a storage medium according to claim 31, wherein: the computer program thereon is configured, when executed, to request a user to input password data as part of the confirmation instructions, and to only permit the terminal to send authentication data once the password data has been input by the user, **[The network users may or may not be given authorization to access or change the exclusion list data entered by the system operator, (Paul et al., Col. 9, lines 52 – 55)].**

Regarding claim 37, an apparatus comprising: at least one server configured to send outgoing electronic messages on behalf of terminals connected thereto and to deliver incoming electronic messages to the terminals, each terminal being accessed by one or more users, **[A plurality of network servers 120, 121, and 122 are coupled to the control center 101 and the communications network 110 as shown in Fig. 1, wherein the servers are mail servers, (Paul et al., Col. 3, lines 57 – 62)],**

the server comprising: means arranged to generate or receive traffic log data based on at least one traffic characteristic using data derived from the handling of plural electronic messages, **[Once the information contained in the received e-mail message is identified and received by processor 104, wherein the received e-mail contains information that is used to filter the e-mails based on the information received, (Paul et al., Col. 5, lines 1 - 6)],**

analyzing means arranged to analyze the traffic log data as a function of a predetermined traffic characteristic criterion corresponding to malicious electronic message traffic to identify electronic messages that satisfy the traffic characteristic criterion, **[Upon receipt of incoming mail addressed to the spam probe addresses, the spam control center automatically analyzes the received mail to identify the source of the message, extracts and processes the source data from the received message, wherein the received message is analyzed based on the characteristics that meet the criterion of a spam message, (Paul et al., Col. 2, lines 1 – 5)],**

identifying means arranged to identify the destination of the identified electronic messages, **[users and/or service providers may optionally implement filtering based upon additional exclusion list categories, such as the "TO", "BCC," "CC," and "SUBJECT" e-mail headers and other headers. Filtering may also be based on the contents in the body of the email, wherein the "to" identifies the destination, (Paul et al., Col. 6, lines 7 – 12)],**

and processing means arranged to send a control message to each of the identified destinations requesting suspension of delivery of the identified electronic

messages, **[generating an alert signal incorporating the extracted source data, (Paul et al., Col. 10, lines 4 – 6)]**,

Paul et al. fails to teach that the traffic characteristic criterion including the number of electronic messages from a common user, terminal or other topological position within a time interval,

Barrett et al. teaches that the traffic characteristic criterion including the volume of data passing at a point along a data path or link in a time interval encompassing a plurality of electronic messages, determining whether the electronic data has characteristics of spam may also include counting a number of communications of electronic data that have been received from the sender during a period of time, **(Barrett et al., Paragraph 6)**,

Barrett et al. further teaches determining whether the electronic data has characteristics of spam may also include counting a number of communications of electronic data that have been received from the sender during a period of time, **(Barrett et al., Paragraph 6)**, in order to determine that the electronic data has characteristics of spam to be blocked when the number of messages received from the sender exceeds a threshold number during the period of time, **(Barrett et al., Paragraph 6)**,

It would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify Paul et al. by including that the traffic characteristic criterion including the number of electronic messages from a common user, terminal or other topological position within a time interval, **(Barrett et al., Paragraph 6)**, in order to

determine that the electronic data has characteristics of spam to be blocked when the number of messages received from the sender exceeds a threshold number during the period of time, **(Barrett et al., Paragraph 6).**

Claims 5 – 7 and 16-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Paul et al. (US 6,052,709), in view of Barrett et al. (US 2002/0059454) and further in view of Toyoshima et al. (6,298,349).

Regarding claims 5, 7, 16 and 18, The modified Paul et al. teaches an apparatus according to claim 1, wherein said server includes including: first storage for storing details data relating to such electronic messages, **[The server 120 includes an e-mail server message store 506 for receiving and storing all e-mail messages transmitted within the network 110 and an e-mail filter 504, (Paul et al., Col. 8, Lines 20-25)],**

The modified Paul et al. fails to teach mapping between users and organizational units which users belong to.

further storage for storing a mapping between users and organizational units to which the users belong, the system management program 220 stores names and identifiers (employee numbers) of employees user who belong to this subordinate organization into the personnel-organization database 26**, (Toyoshima et al., Col. 7, Lines 58-62)],** display means for displaying a plurality of images, each representative of an organizational unit, **[FIG. 4 is a drawing illustrating an image displayed on the**

display device 200 in accordance with the group display function of the system management program 220, (Toyoshima et al., Col. 8, lines 6-10), wherein the server is arranged, in use, such that in response to a request for data relating to a user, the first storage is arranged to output data identifying electronic messages emanating from that user, **[The server 120 includes an e-mail server message store 506 for receiving and storing all e-mail messages transmitted within the network 110 and an e-mail filter 504, (Paul et al., Col. 8, Lines 20-25)],** the further storage is arranged to output data identifying which of the organizational units that user belongs to, **[the GUI module 222 outputs data, which is entered by a system administrator via the keyboard 204 or the like, to the database access module 224 and a given one of the GUIs 228, (Toyoshima et al., Col. 7, lines 6-11)],** and, for those electronic messages that are identified to satisfy the criterion, the display means is arranged to insert, on the image corresponding to the identified organizational unit, a visual identifier representative of the volume or type of identified electronic messages, **[in accordance with the network system 1 of this invention, it is possible to visually display subordinate organizations of users in association with constituents of the network system 1, (Toyoshima et al., Col. 12, lines 60-65)],** to provide a system resource display apparatus and a method for use in a network system, comprising a plurality of devices such as computers or the like connected via a network, which are arranged to display information relating to hardware and/or software resources of each of the devices in association with users and organizational groups that possess the devices, **(Toyoshima et al., Col. 1, lines 35-40),**

It would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the modified Paul by mapping between users and organizational units which users belong and displaying a plurality of images, each representative of an organizational unit, **(Toyoshima et al., Col. 7, Lines 58-62),** to provide a system resource display apparatus and a method for use in a network system, comprising a plurality of devices such as computers or the like connected via a network, which are arranged to display information relating to hardware and/or software resources of each of the devices in association with users and organizational groups that possess the devices, **(Toyoshima et al., Col. 1, lines 35-40).**

Regarding claims 6 and 17, an apparatus according to claim 5, wherein: for those electronic messages that are identified to satisfy the criterion, the display means is arranged to display a list of users on an associated image, **[identifying the messages as unsolicited messages by displaying the messages in a distinctive display mode, (Paul et al., Col. 1, lines 45 – 50)],**

and for each user on the list, to display details of the volume and/or type of identified electronic messages emanating therefrom, **[Optionally, the filter 204 may use multiple display codes indicating multiple status levels of "JUNK.", (Paul et al., Col. 6, lines 50 – 53)].**

Claims 35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Paul et al. (US 6,052,709), in view of Barrett et al. (US 2002/0059454) and further in view of Tarbotton et al. (6,757,830).

Regarding claims 35, Paul et al. teaches one server configured to send outgoing electronic messages on behalf of terminals connected thereto and to deliver incoming electronic messages to the terminals, each terminal being accessed by one or more users, an incoming e-mail message is initially received at a remote e-mail server over a network, the incoming e-mail message is transmitted from the remote e-mail sever to the user computer over the network, if it is not blocked, **(Paul et al., Col. 3, lines 57 – 62),**

Paul et al. fails to teach that the criterion is met if traffic tog data corresponding to a target electronic message indicates that a threshold number of electronic messages in a time interval during which the target electronic message was sent,

Tarbotton et al. teaches that FIG. 5 illustrates characteristics of a number of example received e-mail messages and how the rules of FIG. 4 may produce a minimum delay period for each message, **(Tarbotton et al., Col. 8, lines 15-18),** to detect the unwanted properties as soon as an e-mail message is received or whilst it is being stored for the minimum delay period, and then these tests repeated only if they have been updated once the minimum delay period has expired, **(Tarbotton et al., Col. 3, lines 60-65)**,

It would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the modified Paul by including that the criterion is met if traffic tog data corresponding to a target electronic message indicates that a threshold number of electronic messages in a time interval during which the target electronic message was sent, **(Tarbotton et al., Col. 8, lines 15-18),** to detect the unwanted properties as soon as an e-mail message is received or whilst it is being stored for the minimum delay period, and then these tests repeated only if they have been updated once the minimum delay period has expired, **(Tarbotton et al., Col. 3, lines 60-65).**

Claim 20 is rejected under 35 U.S.C. 103(a) as being unpatentable over Paul et al. (US 6,052,709), in view of Barrett et al. (US 2002/0059454) and further in view of Nielson et al. (US 6,453,327).

Regarding claim 20, Paul et al. teaches an apparatus according to claim 1, wherein said server includes including: first storage for storing details data relating to such electronic messages, **[The server 120 includes an e-mail server message store 506 for receiving and storing all e-mail messages transmitted within the network 110 and an e-mail filter 504, (Paul et al., Col. 8, Lines 20-25)],**

Paul et al. fails to teach mapping between users and organizational units which users belong to.

further storage for storing a mapping between users and organizational units to which the users belong, the system management program 220 stores names and

identifiers (employee numbers) of employees user who belong to this subordinate organization into the personnel-organization database 26, **(Toyoshima et al., Col. 7, Lines 58-62)],**

display means for displaying a plurality of images, each representative of an organizational unit, **[FIG. 4 is a drawing illustrating an image displayed on the display device 200 in accordance with the group display function of the system management program 220, (Toyoshima et al., Col. 8, lines 6-10),**

wherein the server is arranged, in use, such that in response to a request for data relating to a user, the first storage is arranged to output data identifying electronic messages emanating from that user, **[The server 120 includes an e-mail server message store 506 for receiving and storing all e-mail messages transmitted within the network 110 and an e-mail filter 504, (Paul et al., Col. 8, Lines 20-25)],**

the further storage is arranged to output data identifying which of the organizational units that user belongs to, **[the GUI module 222 outputs data, which is entered by a system administrator via the keyboard 204 or the like, to the database access module 224 and a given one of the GUIs 228, (Toyoshima et al., Col. 7, lines 6-11)],**

and, for those electronic messages that are identified to satisfy the criterion, the display means is arranged to insert, on the image corresponding to the identified organizational unit, a visual identifier representative of the volume or type of identified electronic messages, **[in accordance with the network system 1 of this invention, it is possible to visually display subordinate organizations of users in association**

with constituents of the network system 1, (Toyoshima et al., Col. 12, lines 60-65)], to provide a system resource display apparatus and a method for use in a network system, comprising a plurality of devices such as computers or the like connected via a network, which are arranged to display information relating to hardware and/or software resources of each of the devices in association with users and organizational groups that possess the devices, **(Toyoshima et al., Col. 1, lines 35-40),**

It would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify Paul by mapping between users and organizational units which users belong and displaying a plurality of images, each representative of an organizational unit, **(Toyoshima et al., Col. 7, Lines 58-62),** to provide a system resource display apparatus and a method for use in a network system, comprising a plurality of devices such as computers or the like connected via a network, which are arranged to display information relating to hardware and/or software resources of each of the devices in association with users and organizational groups that possess the devices, **(Toyoshima et al., Col. 1, lines 35-40),**

The modified Paul fails to teach analyzing means arranged to analyze the traffic log data as a function of a predetermined traffic characteristic criterion corresponding to malicious electronic message traffic to identify electronic messages that satisfy the traffic characteristic criterion,

Nielsen et al. teaches each record 600 in the User's Junk E-mail database contains a "Junk E-mail Characteristics" field 601 and a "Last Date" field 603. The contents of the " Junk E-mail Characteristics " field 601 is associated with a set of text

strings, **(Nielson et al., Col. 9, lines 13 – 20)**, in order to provide a mechanism for identifying and automatically deleting most junk e-mail messages, **(Nielson et al., Col. 3, lines 53 – 55),**

It would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the modified Paul by analyzing means arranged to analyze the traffic log data as a function of a predetermined traffic characteristic criterion corresponding to malicious electronic message traffic to identify electronic messages that satisfy the traffic characteristic criterion wherein Nielsen et al. teaches each record 600 in the User's Junk E-mail database contains a "Junk E-mail Characteristics" field 601 and a "Last Date" field 603. The contents of the " Junk E-mail Characteristics " field 601 is associated with a set of text strings, **(Nielson et al., Col. 9, lines 13 – 20)**, in order to provide a mechanism for identifying and automatically deleting most junk e-mail messages, **(Nielson et al., Col. 3, lines 53 – 55).**

Claims 25 – 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Paul et al. (US 6,052,709), in view of Barrett et al. (US 2002/0059454) and further in view of Khanna et al. (US 2002/0133604).

Regarding claim 25, The modified Paul et al. teaches a server according to claim 1, the server being arranged to receive authentication data from a terminal connected thereto, the authentication data being associated with one or more electronic messages,

[The network users may or may not be given authorization to access or change the exclusion list data entered by the system operator, (Paul et al., Col. 9, lines 52 – 55)],

and the processing means being arranged to execute a decision to send a suspension request to the identified destination of that message in dependence on the comparison made by the comparison stage, **[messages marked with the first display code indicating the "JUNK" status of the message are not displayed in the user's in-box and are automatically discarded by the filter, wherein the alert message discards the electronic message, (Paul et al., Col. 6, lines 65 – 67)],**

The modified Paul fails to teach that the server having configured to make a comparison between traffic log data corresponding to an identified message and the authentication data corresponding to-that message,

Khanna et al. teaches the login unit to incorporate the authentication data in the at least one user entry that corresponds to the at least one instruction set in the instruction set database, wherein the login unit is to store log data related to logging in the user into the web site, **(Khanna et al., Claim 10, Page 8)**, to retrieve the log data from the server, **(Khanna et al., Claim 10, Page 8),**

It would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the modified Paul by including that the server is configured to make a comparison between traffic log data corresponding to an identified message and the authentication data corresponding to-that message, the login unit to incorporate the authentication data in the at least one user entry that corresponds to the

at least one instruction set in the instruction set database, wherein the login unit is to store log data related to logging in the user into the web site, **(Khanna et al., Claim 10, Page 8)**, to retrieve the log data from the server, **(Khanna et al., Claim 10, Page 8).**

Regarding claims 26 and 29, the modified Paul et al. teaches the network users may or may not be given authorization to access or change the exclusion list data entered by the system operator, **(Paul et al., Col. 9, lines 52 – 55),**

The modified Paul et al. fails to teach that the authentication is encrypted,

Steiger et al. teaches a server according to claim 25, wherein: the authentication data is received in encrypted form, **[transmissions may be encrypted so customer data and SOC resources may be protected, (Steiger et al., Col. 9, Lines 45 - 47)],**

the comparison stage being configured to decrypt the encrypted authentication data and to compare the decrypted data with the traffic log data, **[transmissions may be encrypted so customer data and SOC resources may be protected, (Steiger et al., Col. 9, Lines 45 - 47),** in order to adequately protect computer information assets on a full-time basis, **(Steiger et al., Col. 1, lines 47 – 50),**

It would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify Paul et al. by encrypting the authentication as taught by Steiger et al., **(Steiger et al., Col. 9, lines 45 – 47)**, in order to adequately protect computer information assets on a full-time basis, **(Steiger et al., Col. 1, lines 47 – 50).**

Regarding claim 27 and 30, a terminal for sending and receiving electronic messages to and from a server according to claim 25, wherein the terminal has an interface, the interface having: a user input for receiving send instructions to send one or more specified electronic messages to a server, **[A user interface 208 is provided to receive inputs from the user and to display e-mail information to the user, (Paul et al., Col. 6, lines 32 – 35)],**

the user input being configured to receive a confirmation input from the user to confirm the send instructions, **[upon receipt of an electronic mail message addressed to the probe address, (Paul et al., Col. 2, lines 57 – 60)],**

and wherein: in response to the confirmation input, the terminal is configured to send the specified electronic messages towards the server and to send authentication data associable with the specified electronic messages, **[The network users may or may not be given authorization to access or change the exclusion list data entered by the system operator, (Paul et al., Col. 9, lines 52 – 55)].**

Regarding claim 28, a terminal according to claim 27 wherein: the terminal is configured to detect whether a traffic characteristic criterion relating to the specified electronic message is met, **[Upon receipt of incoming mail addressed to the spam probe addresses, the spam control center automatically analyzes the received mail to identify the source of the message, extracts and processes the source data from the received message, wherein the received message is analyzed**

based on the characteristics that meet the criterion of a spam message, (Paul et al., Col. 2, lines 1 – 5)],

and to request a confirmation input from a user at the user interface in response to the criterion being met, **[upon receipt of an electronic mail message addressed to the probe address, (Paul et al., Col. 2, lines 57 – 60)].**

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to **Shaq Taha** whose telephone number is 571-270-1921. The examiner can normally be reached on 8:30am-5pm Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, **Jeff Pwu** can be reached on 571-272-6798.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published

applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free?).

/S. T./

Examiner, Art Unit 2446

/Jeffrey Pwu/

Supervisory Patent Examiner, Art Unit 2446